



Systems Security Engineering Working Group – Is There a Place for Me?

October 17, 2019

Beth Wilson

INCOSE Systems Security Engineering (SSE) Working Group (WG) Co-Chair

Topics

- General Working Group Information
- Systems Security Engineering Working Group
- Is There a Place for Me?

Abstract: *The INCOSE Systems Security Engineering (SSE) Working Group (WG) offers a rich opportunity to engage in the state of the art and practice in systems security engineering. The SSE WG activities are shaping the future, exploring new techniques, collaborating across disciplines and organizations, and developing INCOSE products designed for the systems engineering practitioner. Our working group enjoys a large number of “workers” who are active in projects and “lurkers” who sign up for email information and represent our fan club. This presentation will highlight some of the SSE WG activities and explain how you can get involved in areas of interest to you whether you are a novice or expert in this area.*



General Working Group Information

INCOSE Working Groups

Agile Systems and Systems Engineering Rick Dove / Ron Lyells, Larry Rosser, Kevin Gunn Transformational	Anti-Terrorism International Bill Mackey Application Domains	Architecture M. Wilkinson / R. Martin / A. Kumar / J. Garner Process Enablers	Automotive Alain Daouin / Gary Ruston Application Domains	Competency Cliff Whitcomb / Mimi Heisey Analytic Enablers
Complex Systems Michael Watson Analytic Enablers	Configuration Management Paul Nelson / Dale Brown / Adriana Dlouze Process Enablers	Critical Infrastructure Protection and Recovery M. Korman / J. Juhasz / A. Adabonjoja Application Domains	Decision Analysis Frank Salvatore Analytic Enablers	Defense Systems Karl Geist Application Domains
Digital Engineering Information Exchange John Coleman / Frank Salvatore / Chris Schreiber Transformational	Enterprise Systems W. Donaldson / M. Harmon / K. Nistrup Process Enablers	Global Earth Observation System of Systems (GEOS) Ken Crowder Application Domains	Healthcare Bob Malins / Chris Unger Application Domains	Human Systems Integration Guy Boy Analytic Enablers
Infrastructure A. Kouassi / L. Uden / M. van de Ven Application Domains	Integration, Verification & Validation Jim Armstrong / Russell Kubycheck Process Enablers	Knowledge Management & Ontologies Juan Llorens / Anabel Fraga Transformational	Lean Systems Engineering Arthur Hyde Transformational	MBSE Initiative Mark Sampson Transformational
MBSE Patterns Bill Schindel / Troy Peterson Transformational	Measurement Paul Frenz / Beth O'Donnell Process Enablers	Model-based Conceptual Design Randall Satterthwaite / Robert Lecorchick Transformational	Natural Systems Curt McManara / Randy Arway Analytic Enablers	Object-Oriented Systems Engineering Method (OOSEM) Howard Lykins / Warren Walcott Transformational
Oil and Gas Christopher Bellows / Aisha Pate Application Domains	PM-SE Integration Jean-Claude Roussel / Tina Srivastava / John Process Enablers	Power & Energy Systems Ray Beach / John Juhasz Application Domains	Process Improvement Jeffrey Brown Transformational	Product Line Engineering H. Chale / R. Darbin / C. Krueger Analytic Enablers
Requirements T. Katz / L. Wheatcraft / M. Ryan / R. Zinni / K. Process Enablers	Resilient Systems John Birtis Analytic Enablers	Risk Management Jack Stein / Bob P. Process Enablers	Space Systems David Kaslow / Alejandro Levi Application Domains	System of Systems Alan Harding / Judith Dahmann Analytic Enablers
System Safety Duncan Kemp / Moaghann O'Neil / Russell Kubycheck Transformational	Systems and Software Interface S. Sheard / M. Pafford / E. Klenast / J. M. Transformational	Systems Engineering Case Study Jorg Laik Analytic Enablers	Systems Engineering Quality Management (SEQM) Barclay Brown / Bill Scheible / Hazel Woodcock Process Enablers	Systems Science J. Martin / R. Edson / S. Natarajan Transformational
Systems Security Engineering Rick Dove / Keith Willett / Beth Wilson / Ken Kepchar Analytic Enablers	Telecommunications John Risson / Daniel Spencer Transformational	Tools Integration & Model Lifecycle Management John Nalton / Lonnie VanZandt Transformational	Training Gabriela Coe Analytic Enablers	Transportation Dale Brown / Denis Simpson / David Rojas Application Domains
Value Proposition Initiative Juan Amenabar Transformational	Very Small Entities Robinson Plack / Laporte / Kaffenberger Transformational			

Systems Security Engineering

✉ Rick Dove / Keith Willett / Beth Wilson / Ken Kepchar

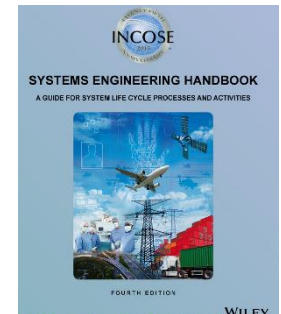
🔗 Analytic Enablers

<https://www.incose.org/incose-member-resources/working-groups/analytic/systems-security-engineering>

What Do Working Groups Do?

• Activities Shape the Future of Systems Engineering

- Explore state of the art
- Define state of the practice
- Influence standards
- Collaborate with related organizations (e.g., NDIA, IEEE)
- Develop content for SE Handbook and SEBoK
- Deliver products to guide practitioners



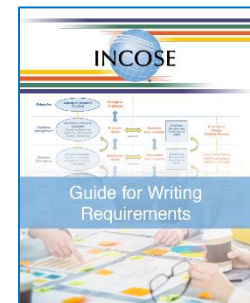
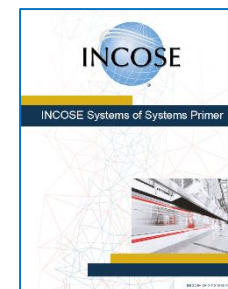
• Products for the Systems Engineering Practitioner

- Webinars
- Tutorials/Papers/Panels at International Symposium
- INCOSE INSIGHT theme issues
- Primers
- Guides

Upcoming Webinars (tentative schedule)

Webinar	Topic	Date
Webinar 1	Practical Model-Based Systems Engineering	October 2018
Webinar 2	Other Systems Engineering (OSSE) Case Studies	November 2018

Webinars will be emailed in advance and international updates will be placed on www.incose.org.
Go to <http://www.incose.org/products-and-publications/webinars> for more info on the webinar series, including a way to view the last 150 Webinars and more – this tool!
Information on the webinars is now being posted in INCOSE Connect, in the INCOSE Library area, at <https://connect.incose.org/Library/Webinars/Pages/INCOSE-Webinars.aspx>.
Joining instructions will be added around two weeks before the webinar is scheduled to take place.



How Can I Find a WG for Me?

- **Drop Into a WG Session in Person**

- International Workshop (longer working sessions)
- International Symposium (short status sessions)



2020
Annual **INCOSE**
international workshop
Torrance, CA, USA
January 25 - 28, 2020



30th Annual **INCOSE**
international symposium
Cape Town, South Africa
July 18 - 23, 2020

- **Explore on the INCOSE Website** (Find Your Community)



<https://www.incose.org>

Working Groups

Systems Security Engineering

Mission & Objectives

This working group's mission is to provide Systems Engineers and Systems Engineering with effective means and methods for sustainable system functionality under advanced adversarial attack.

This working group believes that system engineering cannot succeed without accepting core responsibility for enabling and facilitating effective system security – partly in system requirements, partly in system trade space recognition, but mainly in system thinking applied to concepts of operations and systems architecture. Sustaining system functionality in the face of intelligent determined attack requires self preservation capabilities that adapt and evolve with equal intelligence, determination, and strength of community. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this.

It is fitting for INCOSE to tackle Next Generation Security, as the issues are leading edge systems engineering issues: architecture, systems of systems, self organizing systems, security tradeoffs with human factors, systems thinking – things that are typically high level integrated-system SE issues.

Current system security strategies are inadequate and cannot be fixed by security engineers alone. The reason is evident: attack communities operate as intelligent, multi-agent, self organizing, system-of-systems – with swarm intelligence, tight learning loops, fast evolution, and dedicated intent. With few exceptions, the systems being targeted are alone, senseless and defenseless – relying on outside benevolence for protection, whether this be separate security systems, laws and penalties, or perceived probabilities of being an overlooked target.

This working group's objectives are to instill systems engineering responsibility for sustainable systems functionality in the face of intelligent, determined, and highly competent system adversaries; to facilitate the assimilation and dispatch of that responsibility; and to instigate self-sustaining cross- community involvement between systems engineers, security engineers, and system security standards..

Participants in this working group's projects are developing vanguard critical understandings.

Intended Outcomes

- Fundamental responsibility within systems engineering accepted and integrated.
- ConOps of actionable next-generation security structures and strategies profiled.
- Next-generation-enabling security concepts established in the relevant standards bodies.
- Identification and publication of a relevant body of knowledge appropriate for the Systems Engineering Body of Knowledge (SEBOK).
- Development and maintenance of appropriate contributions to the INCOSE Systems Engineering Handbook .
- Socialization of work efforts with papers for INCOSE's Journal of Systems Engineering, papers and tutorials at the International Symposium, INSIGHT theme issues, and educational and tutorial Webinars.
- Working alliances with other organizations concerned with secure sustainable systems.

AI/ML Systems and Systems Engineering	Anti-Terrorism / International Relations	Architecture	Automotive	Compendex

- Mission & Objectives
- Leadership
- Working Group Products
- Planned Working Session at the Next Events



Systems Security Engineering Working Group

Systems Security Engineering (SSE) Working Group (WG)

- **Purpose:** Identify effective system security principles consistent with new reality; and integrate responsibility into the SE community
- **Goals**
 - SE responsibility for system security
 - SE influence on security and standards
 - SE concepts for next generation security
 - International engagement
- **Scope:** System Engineering enablement of next generation system security strategies: adaptive, resilient, evolutionary



Mission & Objectives

This working group's mission is to provide Systems Engineers and Systems Engineering with effective means and methods for sustainable system functionality under advanced adversarial attack. This working group believes that system engineering cannot succeed without accepting core responsibility for enabling and facilitating effective system security – partly in system requirements, partly in system trade space recognition, but mainly in system thinking applied to concepts of operations and systems architecture. Sustaining system functionality in the face of intelligent determined attack requires self preservation capabilities that adapt and evolve with equal intelligence, determination, and strength of community. This requires full system awareness and adaptability, and system-of-system relationships. Security engineering alone cannot accomplish this.

It is fitting for INCOSE to tackle Next Generation Security, as the issues are leading edge systems engineering issues: architecture, systems of systems, self organizing systems, security tradeoffs with human factors, systems thinking – things that are typically high level integrated-system SE issues.

Current system security strategies are inadequate and cannot be fixed by security engineers alone. The reason is evident: attack communities operate as intelligent, multi-agent, self organizing, system-of-systems – with swarm intelligence, tight learning loops, fast evolution, and dedicated intent. With few exceptions, the systems being targeted are alone, senseless and defenseless – relying on outside benevolence for protection, whether this be separate security systems, laws and penalties, or perceived probabilities of being an overlooked target.

This working group's objectives are to instill systems engineering responsibility for sustainable systems functionality in the face of intelligent, determined, and highly competent system adversaries; to facilitate the assimilation and dispatch of that responsibility; and to instigate self-sustaining cross- community involvement between systems engineers, security engineers, and system security standards..

Participants in this working group's projects are developing vanguard critical understandings.

SSE WG

Operating Principles

- **Objectives:**

- Leverageable fundamentals rather than niche practices & recommendations
- Applied rather than theoretical research
- In-demand knowledge products for the practitioner
- Embraceable knowledge products (a joy to use)
- Testing and refinement to verify efficacy
- Socialization and facilitated-assimilation of results



- **Project Execution**

- Clear project objectives, customers, and plans
- Core members with passionate interest driven by personal value
- Effective project leadership
- Firm deliverable dates
- Frequency & Momentum – project-progress meetings weekly.
- Knowledge-development and remote collaboration tools
- Incrementally releasable deliverables – papers towards INCOSE products
- Reflective process learning
- Oversight progress facilitation

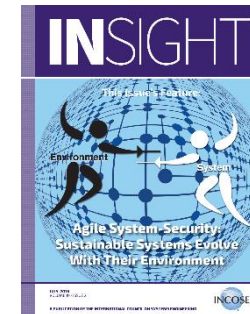
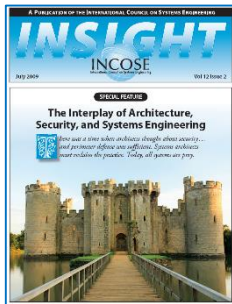


- **Reality:** People work on what they want to work on, but we attempt to guide

SSE WG Completed Projects

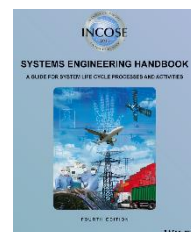
• INCOSE INSIGHT Theme Issues

- July 2009: *Interplay of Architecture, Security, and Systems Engineering*
- July 2011: *Systems of systems and Self-Organizing Security*
- July 2013: *Systems Engineering is Responsible for Systems Security*
- July 2016: *Agile System Security: Sustainable Systems Evolve with their Environment*



• Projects and Products

- SEBoK SSE Content and References
- SE Handbook Content for V4 (SSE and Case Study)
- Security for Continuous Iterative Development (DSB Recommendations)



SSE WG

Ongoing Projects

- **Projects and Products**

- Standards (ISO and NIST)
- Webinars



- **Papers/Panels/Tutorials**

- INCOSE Symposium (summer)
- Non-INCOSE conferences



- **Collaborations (Ongoing)**

- NDIA (SE Division and Cyber Division)
- ABET (Cybersecurity Accreditation)
- INCOSE
 - Resilient Systems WG
 - Critical Infrastructure Protection and Recovery WG
 - Product Line Engineering WG
 - Competency WG
 - Academic Council



SSE WG Current Projects: INCOSE INSIGHT Theme Sep 2020

- Systems Security and Product Line Engineering
- Timeline:
 - Nov 15: Abstracts due
 - Jan 1: Draft papers due
 - IW20: Live review of papers
 - Apr 15: Final papers due

*Exploring Cyber Secure
and
Resilient Approaches
for
Feature Based
Variation Management*



INSIGHT Magazine
"Systems Security and Product Line Engineering"
September 2020 Theme Issue

Call for Articles

Exploring Cyber Secure and Resilient Approaches for Feature Based Variation Management

Mission: The Systems Security Engineering Working Group and the Product Line Engineering Working Group is working a joint project to explore cyber secure and resilient approaches for feature based variation management. This call for articles focuses on the intersection between systems security engineering and product line engineering including:

- Techniques for implementing systems security as part of product line design
- Patterns for product line architectures that address systems security
- Variation management approaches for secure and resilient product line assets

Approach: The Theme Issue will accommodate ten ~2,000 word articles, preceded by a theme introduction and overview. The INSIGHT audience is the Systems Engineering community, who are concerned with systems of multiple engineering domains. Articles should not speak exclusively to a single engineering domain; but rather to a systems engineering audience concerned with the application and adoption of system security engineering and product line engineering concepts across a wide variety of project types.

Schedule

2019 Nov 15: Abstracts Due

Submit declarations of intent and working title, with one paragraph working abstract.

2020 Jan 1: Draft Paper Due

Theme Editor will review for alignment with mission

Live review at IW20 (in attendance or GlobalMeet)

Detailed comments provided to authors for improvement by March 1

2020 Apr 15: Final Paper Due

Formatted for required style, with author-company release if necessary.

INSIGHT editors will contact authors directly with copy-editing suggestions.

2020 September: INCOSE INSIGHT publication

General guidance

- Articles must speak meaningfully to systems engineers
- The INSIGHT style and citation guides will be sent to all authors.
- These are not journal articles. Approximately 2000 words is the target. Reference lists should be minimal.
- Do not use the MS Word reference tool, make them standard text in "Chicago Style", per INSIGHT style guide.
- Acceptance of an abstract does not guarantee publication of an article. Final decision for publication will be made by the Editorial Board based on the final article

Submissions: All submissions should be MS Word, 12 point Times New Roman, single spaced, with minimal or no (preferred) use of styles. With 1 inch margins on 8-1/2 x 11 inch layout this is about 4 pages of text, exclusive of graphics. Graphics are highly encouraged and do not take away from word-count. NO PDF. Send submissions to Theme Editor wilsondbeth@aol.com attached as an MS Word document. Be sure to include a title, and also your name and email address in your by-line underneath the article title.

SSE WG Current Projects: 2020 Systems Security Symposium

- IEEE-INCOS-NDIA SSS

- April 6-8, 2020



2020

SYSTEMS SECURITY
symposium



2020
SYSTEMS SECURITY
symposium

Marriott Crystal Gateway
Crystal City, Virginia, USA
Washington DC area



IEEE SYSTEMS COUNCIL



AESS
IEEE Aerospace &
Electronic Systems Society

CALL FOR PAPERS

IMPORTANT DATES

August 31, 2019
Special Sessions & Tutorial Proposals

September 30, 2019
Initial Papers and Extended Abstracts Deadline

November 30, 2019
Acceptance Notification

CONFERENCE DATES

April 6-9, 2020
Symposium
Marriott Crystal Gateway
Crystal City, Virginia, USA

ORGANIZERS

General Chair
Bob Rassa
IEEE Systems Council
RCRassa@Raytheon.com

Technical Program Chair
Holly Dunlap
NDIA
Holly.Dunlap@raytheon.com

Technical Program Co-Chair
Beth Wilson
INCOS-EE
wilsonbeth@aol.com

Technical Program Committee
Steve Holt
IEEE Systems Council
smhdholt@gmail.com

Kathleen Kramer
IEEE Aerospace & Electronic Systems Society
kramer@sandiego.edu

Tom McDermott
Systems Engineering Research Center
tmcdermo@stevens.edu

Melinda Reed
OUSD (R&E)
melinda.k.reed4.civ@mail.mil

James H. Lambert
University of Virginia
lambert@virginia.edu

Logan Mailloux
United States Air Force
logan.mailloux@us.af.mil

The IEEE-INCOS-NDIA Systems Security Symposium seeks research papers and application studies that focus on the development of secure, safe, and resilient systems. This symposium attempts to address the convergence of cybersecurity, safety, and engineering with interest in the effective application of security principles, methods, and tools to complex systems such as cyber-physical systems, autonomous systems, transportation vehicles, medical devices, large IoT systems, and other systems of interest. Preference will be given to papers and case studies that bridge theory to practice.

THEORY & METHODS

Papers or Extended Abstracts addressing novel ideas, theoretical issues, technology, methodology, or detailed studies. These academic-oriented papers will be peer reviewed and prioritized according to their contribution.

CASES & PRACTICAL EXPERIENCES

Papers presenting practical ideas, lessons learned, and real-world achievements. Papers are reviewed for relevance but not necessarily academic contribution.

Papers and extended abstracts of both categories will be peer reviewed. Papers will be published in the proceedings with an 8-page maximum. Extended abstracts (typically 3-5 pages) will not be published, but will be available to the conference attendees. Student papers are encouraged in both categories.

All submission details are available on the IEEE-INCOS-NDIA SSS 2020 Submission Portal at
<https://2020.ieeesystemssecuritysymposium.org>

Tutorials (1/2 day) are encouraged; please add TUTORIAL to your paper title. Best Paper monetary awards will be recognized for professional and student papers. Table top exhibits are available on a first come, first serve basis. See website for details.

AREAS OF INTEREST

» Systems Security Work Focused on Advancements in Theory, Practice, & Education » Engineering of Safe, Secure, & Resilient Systems » Examples of Mission/Systems Assurance & Assurance Cases » Model Based Engineering Focused on Security, Safety, Trust, Resiliency » Affordable & Scalable Approaches to Hardware, Software, Firmware Assurance » Novel Architecture Design & Analysis Examples or Trade-Space Studies » Trust of Complex Systems with Emphasis on Cyber-Physical Systems » Security Considerations for Machine Learning / Artificial Intelligence » Large-Scale DevSecOps & Agile Approaches for System Development » Verification, Validation, & Evidences for Secure System Development	» System Security Design Considerations for Cloud Environments » Extensions of Formal Methods to System-Level Evaluation » Cybersecurity in Manufacturing & Supply Chains » Case Studies to Include Automotive, Transportation, Space, & Others » Cyber-Physical System Event Detection, Investigation, Forensics, & Malware Analysis » Tailored Risk Management Approaches for Large Complex Systems » Attack/Defense Modeling, Simulation, & Characterization » Techniques for Cyber Risk Buy Down in Legacy Systems, Infrastructure, & Enterprises » Policy, Ethical, Legal, Privacy, Economic, & Social Issues
---	--



IEEE
Advancing Technology
for Humanity



INCOS-EE



SYSTEMS
ENGINEERING
RESEARCH CENTER



NDIA



UNIVERSITY
OF VIRGINIA

SSE WG Current Projects: Systems Security/Product Line Design

- **Project Objective:** Bring systems security into product line design
 - **Goal:** Identify techniques for implementing systems security as part of product line design
 - **Goal:** Identify patterns for product line architectures that addresses systems security
 - **Goal:** Identify variation management approaches for secure and resilient product line assets
- **Notional Examples**
 - Maritime Search and Rescue Mission
 - Connected Car
- **Sub-Team Efforts**
 - Resiliency Techniques for SE Products
 - Non-Traditional Application of PLE
 - Cyber Resiliency Techniques for PLE
 - Rule-Based Approach to Validate Variants
 - Quantify Benefit of SSE in PLE
 - Requirements Flow-Down from PLE to Solutions
 - Alignment with PLE and SSE Standards
 - Identify Patterns for Cyber-Resilient Product Line Architectures
- **Planned Deliverables**
 - INCOSE INSIGHT Q3 2020
 - Papers at IEEE-INCOSE-NDIA SSS 2020
 - INCOSE webinar



***Cyber Secure and Resilient Approaches
for Feature Based Variation Management***

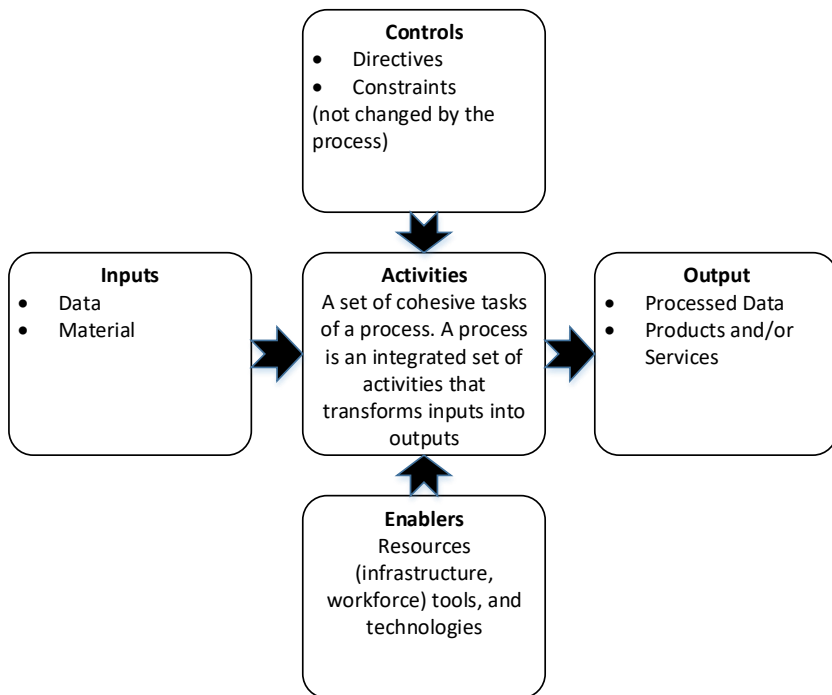
SSE WG Current Projects: SSE/SE Roles and Responsibilities

• SSE/SE Roles and Responsibilities Framework Project

- Responsibility and Artifact Framework
- Align with NIST 800-160

- **SE Handbook V5**

- Adapt V4 content
- Integrate framework into handbook update

[illegible]

SSE WG Current Projects: Security in the Future of SE (FuSE)



FuSE Collaborative Community



FuSE Road Map



SSE WG Working Group Awards

- **2013:** Sustained Performance
- **2016:** Collaboration



*"We are delighted to confirm that the Systems Security Working Group has been selected to receive a **2016 award for Collaboration**. This award is intended to recognize the Systems Security Working Group for collaborating with National Defense Industrial Association (NDIA) and the National Institute of Standards and Technology on NIST Special Publication 800-160."*

*"We are delighted to confirm that the Systems Security Engineering WG Team has been selected to receive a **2013 award for Sustained Performance**. This award is intended to recognize the group for providing exemplary value to INCOSE stakeholders in raising awareness of a critical topic and making contributions to Systems Security Engineering over the past four years in three specially themed issues of INCOSE INSIGHT, organizing security panels at International Symposia, and new contributions to the INCOSE Systems Engineering Handbook."*



Is There a Place for Me?

How to Engage with Working Groups

- **Workers (Active Members)**

- Attend WG meetings at IW and IS (in person, some have virtual options)
- Volunteer to participate in or lead a project
- Volunteer to be a reviewer (products, INSIGHT, IS papers, standards drafts)



- **Lurkers (Fan Club)**

- Join WG and check out activities
- Sign up for email information
- Attend WG meetings or just read the notes that come out after
- Use WG products



How Do I Benefit?

- **Learn New Things**

- Find out about new initiatives
- Explore new techniques



- **Career Advancement**

- Publication opportunities
- Connections to experts and mentors



- **Even in Retirement**

- Keep current in the Systems Engineering field
- Contribute to and learn from practitioner products





SSE WG is waiting for you!